Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1716 04/17/15

~ Welcome to Dark Side! ~ People Are Talking! ~ House of Wolves!
~ Lawmaker Gets Swatted! ~ Memex A Google-killer? ~ US Cops Pay Ransom!
~ GameStop Goes Classic! ~ Battlezone to the PSP! ~ ISP's Want Names!

~ XP Clings to #2 Spot! ~ Auto-squash the Trolls ~ WoW Gold Trading!

-* Hackers Fight Cyber Attacks! *-
-* More Suits Against Net Neutrality! *-
-* Teen Charged for Using Teacher’s Password! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
  """""""""""""""""""""""""""""

It’s getting late, so I’ll not talk about the long-awaited terrific stretch of nice weather this week, or the extensive high-profile criminal trials in the area. Instead, we’ll just move right along.

Until next time...

=~=~=~=

->In This Week’s Gaming Section - No Raid in Second Destiny Expansion House of Wolves!
  """"""""""""""""""""""""""""""" Atari Classic Battlezone Coming to PSP!
  GameStop To Offer Classic Consoles and Games!

  And more!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
  """""""""""""""""""""""""""""""""""""

Bungie: No Raid in Second Destiny Expansion House of Wolves

There will be no raid in the House of Wolves, the second expansion pack for Bungie s massively-multiplayer first person shooter Destiny, the developer has confirmed.

Instead, high-level players will be treated to a three-player co-operative experience focused on variety, replayability, and skill a new battle arena called The Prison of Elders, Bungie says.

The arena will be for three players, rather than the six who are required to play one of Destiny s two raids, and is paired with a new competitive

multiplayer mode called Trials of Osiris. Both will be available to play upon the release of the second expansion pack on 19 May.

Destiny, which fuses the FPS mechanics of games such as Bungie s previous hit Halo with the trappings of a massively multiplayer online game such as World of Warcraft, currently has two raids as end-game content, available to players who have already mastered much of what the game has to offer.

The first, the Vault of Glass, was introduced a few weeks after the game debuted, and required a team of six high-level players to independently form a team and defeat the god of the machine lifeforms known as the Vex.

It was praised for introducing innovative new mechanics to a game which was, in the words of Guardian reviewer Keith Stuart, a highly conventional old-school shooter , but criticised for being largely inaccessible to casual players, requiring a large time commitment to reach the prerequisite level and an equally large commitment to put together a team and take on the challenge.

That raid was followed in December with Crota s End, released as part of the game s first expansion pack The Dark Below, and players had expected House of Wolves to introduce a third raid.

GameStop To Offer Classic Consoles and Games

Dust off your Nintendo 64. Once again it, and other retro consoles, will be accepted at GameStop. The company will launch a pilot sales and trade-in program for retro consoles, games, and accessories in two of its markets beginning April 25.

Stores in its NYC and Birmingham markets, which comprise around 250 store locations, will play host to the program.

According to a spokesperson for GameStop, the qualifying locations will begin accepting "games, systems and select accessories for most ’retro’ platforms," going all the way back to the Nintendo Entertainment System. If the program proves successful, GameStop hopes to roll it out nationally "later this year."

This will increase the number of games GameStop offers either for sale or to purchase by "about 5000."

The systems and accessories that you will be able to trade-in and purchase include the NES, Super NES, SEGA Genesis, PlayStation, N64, and SEGA Dreamcast. This will increase the number of games GameStop offers either for sale or to purchase by "about 5000."

"We will bring all of the product back through the Refurbishment Operations Center for inspection, testing and repair," GameStop told us. The lead time between when it begins accepting trades and when the products will be put on sale is estimated to be about 2 months. This gives the company sufficient processing time and "time to build up a good assortment for retro games fans to select from when shopping."

However, you won’t be inundated with the sights and sounds of your favorite retro games when you walk into your local store. Purchases can

be made on GameStop’s website or through its web-in-store system.

The GameStop spokesperson said all of these retro consoles are expected to "have the same warranty as current used and refurbished consoles."

Earlier in the year, a report surfaced that GameStop had developed a system to repair the dreaded red-ring of death problem in Xbox 360 consoles, a report that was later verified in a statement from the company.

At the beginning of March, GameStop announced it would once again start accepting PlayStation 2 consoles for in-store credit.

Dollar s Buying Power Plummets in First Day of Official WoW Gold Trading

Just over a day after Blizzard introduced the first official method for converting dollars into World of Warcraft gold, the amount of in-game currency you can get for real-world cash has already plummeted 27 percent from the initial position set by Blizzard.

For most of World of Warcraft’s history, the only way to buy in-game gold with real currency was to go through one of many gray market third-party services (which technically goes against Blizzard’s terms of service for the game). That was true until yesterday, when Blizzard introduced a $20 game time token that can be sold for gold at the in-game auction house on North American servers (European servers will get the feature at a later date). While the real-world price of those tokens is fixed at $20, the gold price is "determined dynamically based on supply and demand," as Blizzard puts it.

To start the market off, Blizzard set the price of a $20 token at 30,000 gold. That gold price increased incrementally for a few hours before plummeting precipitously starting yesterday evening in the US. As of this writing, just over 24 hours after the markets opened, that initial gold price of a token has fallen over 27 percent to 21,739 gold, according to an API-based tracking site.

This isn’t that surprising when you look at the going rates for WoW gold from third-party sellers. According to wowgoldrates.com, $20 can get you anywhere from 10,000 to roughly 15,000 gold on the gray market, depending on which reseller you use (you can get slightly better rates if you buy in bulk).

Blizzard’s initial 30,000 gold price for a $20 token was two to three times more generous than those prevailing rates, from the gold buying perspective, and had the added benefit of operating under Blizzard’s official approval. This led gold buyers to predictably flood the in-game auction house with available tokens, driving the price steadily downward. Players that realized the market skew early reaped a much greater windfall than those that got into the market even a few hours later (Don’t worry about resellers trying to game the market by buying low and selling high, though once a token is purchased from the auction house with gold, it can’t be resold).

By selling monthly game subscriptions for in-game gold, the WoW token also has the interesting side effect of setting an indirect value on subscriptions in terms of in-game time spent grinding for gold. Some

dedicated high-level gold farmers report making 2,000 to 4,000 gold per hour with focused money-making techniques, meaning a month’s worth of WoW time can currently be sustained with about 6 to 11 hours of grinding.

With direct purchases of subscriptions running just $15 a month, that kind of grinding isn’t really a great monetary return on the time investment (unless you’re working from a very economically depressed area of the world). Still, it’s not an awful trade for players low on spending cash but heavy on time to waste playing WoW. And that’s not even considering the more outrageous farming tutorials that promise rates of return up to 10,000 gold per hour.

The drop in auction house token prices seems to be slowing down somewhat today, after last night’s more severe drop. Still, it seems likely that the "official" gold value of a dollar will continue to decline until it at least approaches the rates already available outside the game. So if you have a hankering to convert some of your excess hoard of gold into some extra play time, we recommend waiting at least a little bit. If you’re looking to turn your money into in-game gear, though, you’d best jump in while the market still seems to be a bit artificially inflated.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Atari Classic Battlezone Coming to PSP

Atari continues to crank out the hits.

The latest triumph for the retro-yet-futuristic company is the development of the classic arcade game BattleZone for PSP. Now you can direct your hover tanks and other high-powered weapons in single-player or multi-player mode.

You can fight it out in the desert canyons of the U.S., the jungles of China, the frozen tundra of Antarctica, and other exciting scenarios. Game modes include Capture the Flag, Hotzone, Knockout, Fox and Hound, Deathmatch, and Team Deathmatch.

You can also use that PSP (and a USB connection) to download upgrades, news, leader boards, customizable game maps, and a host of other add-ons.

You ll have to wait a bit, though. BattleZone for PSP is expected to be available for purchase in November.

=~=~=~=

A-ONE’s Headline News

The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Suit Filed as US ’Open Internet’ Rule Becomes Official

A telecom industry group Monday challenged "open Internet" regulations barring US broadband providers from separating online traffic into slow and fast lanes, hours after official publication of the order.

The US Federal Communications Commission published its "net neutrality" order in the federal register earlier Monday, making the hotly contested rules effective June 12.

USTelecom, a trade group that includes major broadband providers such as AT&T and Verizon, announced it had filed a lawsuit in federal court seeking to block implementation of the plan.

USTelecom president Walter McCormick said the FCC order is an "unjustifiable shift backward to common carrier regulation" and that the plan "slows innovation, chills investment, and leads to increased costs on consumers."

The FCC’s 3-2 vote in February in favor of so-called "net neutrality" followed an intense debate in Washington pitting backers of online services like Netflix, Twitter and Yelp against big Internet service providers like AT&T and Verizon.

The ruling, on the heels of a long regulatory court battle, sets a new standard that treats all Internet traffic as equal, preventing Internet firms from charging fees for better access.

Backers said the move guarantees Internet users can roam freely online and prevents any effort to stifle expression, but critics complained it would give the government too much control.

The new challenge means the case goes back to federal court just more than a year after an appellate panel struck down a similar order saying the FCC lacked jurisdiction to enforce net neutrality.

The FCC rewrote the rules, this time by reclassifying broadband as a "public utility" under a 1934 telecom law.

Backers of the new rule say it is needed to prevent big broadband firms from locking out new services which cannot or will not pay for "fast lane" service. But critics say it amounts to old-style regulation that lacks relevance in the digital era.

The trade group and a small Internet firm announced last month they were challenging the order but officials said courts would not hear the case until the official publication of the rules.

The rules could also face obstacles in Congress where several Republican lawmakers have called for the plan to be stopped.

Republican Representative Doug Collins on Monday introduced a "resolution of disapproval" to void the FCC rules, arguing that the plan would have the opposite effect of its intent, and could lead to slower Internet

speeds and higher costs.

"Resources that could go to broadband deployment will go to federal taxes and fees, he said in a statement in introducing the measure with 14 co-sponsors. "We ll all be paying more for less."

But Chris Lewis at the activist group Public Knowledge argued that the FCC rule reflects "a large and growing bipartisan consensus that simple, strong rules are important to protect an open Internet" and that without the plan "consumers may see the digital divide increase."

FCC Faces Seventh Net Neutrality Lawsuit

Broadband provider CenturyLink has joined the list of ISPs and trade groups suing the U.S. Federal Communications Commission over its net neutrality rules.

CenturyLink filed its lawsuit Friday, becoming the seventh organization to challenge the rules approved by the FCC in late February. The FCC officially published the rules in the Federal Register, the official publication for U.S. agency rules, earlier this week, prompting a round of lawsuits.

The company objected to the FCC’s reclassification of broadband from a lightly regulated information service to a more heavily regulated common-carrier service. CenturyLink spends hundreds of millions of dollars a year to "build, maintain and update an open Internet network and does not block or degrade lawful content," it said in a statement.

The common-carrier regulations, dating back to the 1930s, "not only have no place in the 21st century economy, but will chill innovation and investment," the company added.

The FCC is confident it will prevail in the lawsuits, Chairman Tom Wheeler said Friday.

CenturyLink, based in Monroe, Louisiana, is the third-largest telecom carrier in the U.S. It acquired Qwest in 2011, and it has about 5 million broadband customers, with its presence the strongest in the U.S. South, Mountain West and parts of the Midwest.

The six other lawsuits come from two ISPs - AT&T and Alamo Broadband - and trade groups CTIA, the United States Telecom Association (USTelecom), the National Cable and Telecommunications Association and the American Cable Association. Alamo and USTelecom filed lawsuits in late March, with the trade group refiling its suit on Monday. AT&T and the three other trade groups filed lawsuits on Tuesday.

The new net neutrality rules, approved by the FCC on Feb. 26, would prohibit broadband and mobile carriers from selectively blocking or slowing Web traffic. The rules reclassify broadband as a regulated telecom service, instead of treating it as a lightly regulated information service, as the FCC has done for the past decade.

Security Companies Hire Hackers, Ex-Spies to Fight Cyber Attacks

Just ask Scott Davies, 30, who left a career snooping on Australia's enemies in December for a similar gig at FireEye Inc. Or Brian Varner, 35, who swapped a job with the U.S. Department of Defense breaking into networks in the Middle East and other hot zones to be a security engineer at Symantec Corp.

"I have a blank canvas to paint whatever I want," says Varner, exulting at the lack of bureaucracy, not to mention his ability to work remotely from Florida.

All told, cybersecurity companies have hired hundreds of ex-government sleuths in recent years, capitalizing on the boom in business caused by hackers who stole more than 1 billion records in attacks last year. The former spies, cyber-warriors and government-groomed hackers are becoming the cornerstone of the cybersecurity services industry, which is projected to bring in more than $48 billion in revenue next year, up 41 percent from 2012, according to Gartner Inc.

"The people coming out of the military and the intelligence community are really, really good," says Nir Zuk, co-founder of Palo Alto Networks Inc. and himself a former Israeli army computer hacker. "They know the attackers. They know how they work."

FireEye has hired more than 100 ex-government hackers since 2013, part of an international expansion that has cost more than $1 billion, according to Chief Executive Officer Dave DeWalt. Symantec has increased the size of its security services division by almost a third, to 500 people, in the past year.

Even smaller companies are snagging top talent. Lacoon Mobile Security, a mobile-security startup that Check Point Software Technologies Ltd. agreed to buy this month, has hired 15 people from Israel's Unit 8200, said Michael Shaulov, a Lacoon co-founder who, like Zuk, served in the Israeli military's computer-hacking group. The hires usually had five to eight competing offers and each earned more than $100,000 straight out of the armed services, Shaulov said.

"There's a bit of a run on security talent," said Rob Owens, an analyst at Pacific Crest Securities in Portland, Oregon, who has covered the industry for almost 20 years.

While CVs that include government hacking can supercharge careers, they're not a guarantee of safety - or an easy fit in corporate America.

Bloomberg reported in February that JPMorgan Chase & Co. has put two former Air Force colonels in its cybersecurity division and that they clashed with the FBI, Secret Service and some members of their own staff about their insistence that Russia's intelligence services were behind a hacking attack on the bank last year. Law enforcement has determined the attack was the work of ordinary cyber-criminals, and insiders said the clash was an example of how military training can cause some to see state-sponsored attacks where there are none.

At Palo Alto Networks, one of Zuk's recent hires was Chief Security Officer Rick Howard, who spent more than two decades in the U.S. Army. He last served as chief of the computer emergency response team before entering the private sector. The $1 billion FireEye has spent on expansion is on top of the 2013 acquisition of Mandiant, a data-breach

investigations company, which was founded by former Air Force special agent Kevin Mandia. That deal was valued at $1.05 billion.

Some investors have been leery of the costs of the added headcount.

FireEye spends 48 percent of revenue on research and development, the highest ratio of any of the 31 companies in the ISE Cyber Security Index, according to data compiled by Bloomberg. The index average is 18 percent.

While FireEye's shares fell from a high of $95.63 in March of last year to a low of $25.76 in October, in large part because of concerns about spending, the stock is up more than 30 percent this year amid signs that DeWalt's pitch to investors is gaining some traction.

"The costs are so much bigger now for the security industry than they ever were - the threat landscape has changed so much," DeWalt said. "You can't just have a product. You need the people to match it. There's no shiny bullet that does it all."

Welcome to the Future: US Cops Pay Bitcoin Ransom To End Office Hostage Drama

Blundering cops in Maine, US, have enriched malware masterminds by paying up to decrypt files held hostage by ransomware.

Four city police departments and a sheriff's office in Lincoln County share a common computer network run by Burgess Computer, which hosts the plods' administrative files.

Then one day the entire system was encrypted by the Megacode ransomware, which scrambles documents and demands Bitcoins to decrypt them.

This sort of malware typically scans computers and networks for documents, generates a random encryption key per file, uses those to encrypt the data, and then encrypts the keys using a public-private key pair. Only the crims have the private key needed to unscramble the documents, and it costs money to obtain that, effectively holding the information to ransom. Victims have a few days to pay up before the private key is deleted forever.

After trying to restore the encrypted files for a couple of days, the police in Maine decided to pay the $300 ransom in Bitcoins.

"Paying a ransom - let's say it goes against the grain," Sheriff Todd Brackett told the Boothbay Register. "We tried to find a way around it, but in the end our IT guys and Burgess recommended just paying the ransom."

The infection kicked off when someone on the police network ran an executable downloaded from the web via a link in an email, it's believed. This installed the malware, which spread to the main server and began encrypting all the data it could find.

"We'll have more virus protection training where we go over how to tell if something might be a virus," Brackett said. "Sometimes, it's hard to tell, but you've got to keep an eye out for some of these documents that people [email] you. Sometimes it can be hard to tell if it contains a virus."

The normal way of dealing with ransomware is a complete disk wipe followed by a reloading of offline backup files, but in this case the backup system hadn’t worked properly, so the cops had no choice but to pony up the digital cash.

"No personal data was mined - it looks like they didn’t take any information," Brackett said. "We had to pay the ransom, but it looks like nothing was extracted from the server."

While the infection has caused red faces, Maine’s police are not alone in getting caught out by ransomware. Cops in Massachusetts were forced to pay up in a similar situation last week, and it’s not the first time they have been stung.

The problem with ransomware is getting much worse these days, as malware writers have cottoned on to the fact that it’s easier to get paid a ransom rather than have to go through all the tricky business of stealing identities from stolen information, or risk selling that information on forums.

The FBI is now offering millions in reward money to catch the crooks behind some ransomware. That’s cheaper than funding police ransom payments, but giving criminals money isn t a long-term solution.

In the meantime, never, ever execute an attachment or download from an untrusted source.

The NSA Wants A Multi-part Encryption Key for "Front Door" Access to Your Data

The US National Security Agency (NSA) appears to be increasingly concerned about the growing adoption of encryption and its ability to thwart the agency’s surveillance efforts.

Now, after months of debate with tech firms about government access to encrypted data on smartphones and other devices, the NSA has proposed a solution which it hopes will strike a balance between its desire to know everything about everyone and the average law-abiding citizen’s right to privacy.

According to The Washington Post, that solution - put forward by NSA director Michael S. Rogers - lies in a multi-part encryption key, created by various tech companies, which could unlock any device.

Speaking at Princeton University recently, Rogers said the key could be broken into several parts, meaning no one agency or company would be able to use it without the co-operation of the others:

I don’t want a back door. I want a front door. And I want the front door to have multiple locks. Big locks.

With the highly contentious Section 215 of the Patriot Act - legislation that has allowed mass eavesdropping from the security services - due to sunset on 1 June 2015, privacy rights groups and concerned members of the public have long been voicing their concerns about bulk data collection.

Add to that the fact that firms such as Apple, Google and Microsoft recently sent a letter to President Barack Obama which demanded an end to data collection, and you can probably see why the NSA is exploring more palatable alternatives.

The debate about encryption and government access comes about as tech companies continue to make customer privacy a key selling point for their products and services.

Companies like Apple - which recently took the decision to enable device encryption by default and made key promises to its customers concerning their privacy - are giving the NSA a real headache as the agency argues the need for government access to data to aid in the battle against crime and terrorism.

Edward Snowden, for his part, continues to lament the level of access the US government still has. At a secret meeting at this year’s South by Southwest festival he urged tech companies to foil surveillance efforts through the development of better privacy tools.

But Rogers firmly believes that his proposal for a ’front door’ is both sound and justified, allowing for access as and when required, while keeping data safe from would-be hackers and other forms of attack.

Of course, his view is not universally shared - Donna Dodson, chief cyber›security adviser at the Commerce Department’s National Institute of Standards and Technologies pointed out that a master key still presents a risk, even if it is broken into parts held by different parties:

The basic question is, is it possible to design a completely secure system? There s no way to do this where you don t have unintentional vulnerabilities.

Privacy advocates and industry officials alike are not convinced by Rogers’ proposal either. Marc Zwillinger, a former Justice Department official now working as an attorney for tech companies on encryption-related matters, told the Post that law enforcement should not have the undeniable right to access every means of communication between two parties. He added:

I don t think our Founding Fathers would think so, either.

The fact that the Constitution offers a process for obtaining a search warrant where there is probable cause is not support for the notion that it should be illegal to make an unbreakable lock. These are two distinct concepts.

Toxin-buying Teen Finds Police Waiting for Him on the Dark Side

Many people use the internet to shop online and take advantage of low pricing, a huge amount of choice and greater convenience.

But not all online purchases are what we would consider to be mainstream - our previous stories about Silk Road and similar marketplaces demonstrate a darker side to the web where people can buy just about anything from drugs to the services of professional hitmen.

This shady part of the net - known as the dark web - has traditionally been out of bounds for law enforcement but, as the closure of Silk Road showed, that is beginning to change.

That was certainly the case when a 16-year-old boy from Manchester, UK, went looking for a deadly toxin and found the police waiting for him on the dark web.

Appearing before Manchester Youth Court on 8 April, the teenager pleaded guilty to attempting to acquire a biological toxin or agent contrary to the Criminal Attempts Act 1981 and section one of the Biological Weapons Act 1974.

The toxin in question - Abrin - is found in the seeds of the rosary pea and castor oil plant and, like ricin, is a ribosome inhibiting protein. It is considered 30 times more toxic than ricin.

Even though an earlier court hearing had been informed that a mere 0.05 milligrams of Abrin was sufficient to kill a human being, the boy’s lawyer argued that he intended to buy 10 milligrams to commit suicide.

The case came about after law enforcement officers informed the North West Counter Terrorism Unit (NWCTU) that they were covertly communicating with the 16-year-old over the dark web, explaining that he had expressed an interest in purchasing the toxin.

The NWCTU was advised on 23 January that the boy was aware that the drug was highly toxic and could be used to cause massive harm.

The teen went on to place an order on 6 February and made it known that he was interested in purchasing subsequent larger quantities.

On 16 February, search warrants were issued and police descended upon two addresses in the Tameside area of Manchester. Two arrests were made, though a 16-year-old girl was later released without charge. The teenage boy is due to be sentenced on 20 April 2015.

Of course it’s not only toxin-buying teenagers finding the police lying in wait on the dark web - in the recent past we’ve seen the likes of Silk Road wannabee Utopia shuttered within a week of opening after it was infiltrated by undercover agents.

And, in November 2014, we saw law enforcement infiltrate the Tor network as a prelude to a multi-nation take down of over 400 "hidden services".

While that sting, dubbed Operation Onymous, only netted 17 arrests, it does provide further evidence that police forces around the world are becoming increasingly proactive in their attempts to bring down the dark web from within.

European Union Accuses Google of Violating Antitrust Laws

The European Union has once again thrown the gauntlet down on Google, this time charging the company with violating antitrust laws by using its dominance in search by favoring its own comparison shopping service at the expense of others. The EU is also launching a separate investigation to see if Google has used its clout as the dominant supplier of mobile phone

software to hold back providers of competing mobile operating systems, namely Apple and Microsoft. Google denied both allegations.

Regarding the charges that it skews results in its search engine to benefit its own shopping comparison service, the EU charged that "Google gives systematic ’favourable’ treatment to its comparison shopping product (currently called ’Google Shopping’) in its general search results pages, e.g. by showing Google Shopping more prominently on the screen."

Google diverts traffic from competing comparison shopping services obstructing their ability to compete, said the EU complaint.

"The Commission is concerned that users do not necessarily see the most relevant results in response to queries - this is to the detriment of consumers, and stifles innovation," it said in a statement. The EU wants Google to operate its own comparison shopping services the same as it treats those of rivals. Google has 10 weeks to respond, at which point the EU will hold a formal hearing.

In response to that allegation, Google said in a blog post it has plenty of competitors and argued its own offerings are often underdogs. "Indeed if you look at shopping - an area where we have seen a lot of complaints and where the European Commission has focused in its Statement of Objections - it’s clear that (a) there’s a ton of competition (including from Amazon and eBay, two of the biggest shopping sites in the world) and (b) Google’s shopping results have not harmed the competition," Amit Singhal, senior vice president of Google Search, said in a blog post. "Companies like Facebook, Pinterest and Amazon have been investing in their own search services and search engines like Quixey, DuckDuckGo and Qwant have attracted new funding. We’re seeing innovation in voice search and the rise of search assistants - with even more to come."

As for Android, the EU said it’s investigating whether or not Google has violated antitrust regulations by thwarting development of mobile applications to other operating system providers by providing incentives to smartphone and tablet suppliers to install Google’s apps and services exclusively. "Distribution agreements are not exclusive, and Android manufacturers install their own apps and apps from other companies as well," said Hiroshi Lockheimer, Google’s VP of engineering for Android, in a blog post addressing the investigation. "And in comparison to Apple - the world’s most profitable (mobile) phone company - there are far fewer Google apps preinstalled on Android phones than Apple apps on iOS devices."

White House Hackers Accessed Schedule of President Obama’s Whereabouts

Since the cyber intrusion into the White House was first discovered in October, the US government has said that ongoing cyber breaches into the president’s executive office network - suspected to come via the US State Department’s system - have only affected an unclassified system.

But it turns out that that’s been enough for the attackers to intercept sensitive information including the president’s whereabouts, in real-time, throughout the day - information that’s not public.

Officials told CNN that in spite of the information being unclassified,

it’s still highly sensitive data that’s prized by foreign intelligence agencies.

The intrusion was first discovered in October, when suspicious activity was detected in the unclassified network that serves the executive office of the president.

Staffers were forced to deal with temporarily disrupted services, having to change passwords, and periodic ongoing shutdowns to allow for security upgrades.

Fingers have pointed at Russia from the get-go, given circumstantial evidence such as reports of cyber-espionage campaigns launched by Russian operatives thought to be working for the government.

One such was Sandworm: a zero-day exploit that was transmitted via Powerpoint files and that took advantage of a previously unpatched Windows vulnerability.

Sources told the Washington Post back in October that the nature of the target - i.e., a government network - is consistent with a state-sponsored campaign.

Investigators - including agents from the FBI, Secret Service and other intelligence agencies - reportedly consider the attack to be among the most sophisticated ever to be launched against US government systems.

As is common, the attack has been routed through computers around the world, making it difficult to pinpoint its origin.

National Security Council spokesman Mark Stroh did say that the government takes this - or any incident like it - "very seriously" but wouldn’t confirm or deny that the government thinks that Russia’s behind it.

CNN quotes him:

In this case, as we made clear at the time, we took immediate measures to evaluate and mitigate the activity. As has been our position, we are not going to comment on [the CNN article’s attribution] to specific actors.

Linux Australia Gets Pwned, Rooted, RATted and Botted

Linux Australia had a bit of a nightmare Easter Weekend.

While the rest of us were loafing at the beach, the Penguinistas from Down Under were owning up to a pretty extensive cyberintrusion.

The team has published a decent document setting out what happened, and it went something like this:

Crooks broke into the organisation’s Conference Management server.
Crooks got root on the server.
Crooks installed a remote access Trojan (RAT) for later.
Crooks rebooted the server and activated the RAT.
Crooks "logged in" again and installed zombie malware, also known as a bot.
While the crooks had access, a conference database backup took place to

the server.

Ironically, the backup that was intended to deliver one leg of the "security trinity" (availability) ended up hurting one of the other legs (confidentiality).

That’s because the database dump as good as dropped a bucket-load of Personally Identifiable Information (PII) in the crooks’ laps:

The database dumps which occurred during the breach include information provided during conference registration - First and Last Names, physical and email addresses, and any phone contact details provided, as well as a hashed version of the user password.

Fortunately, payment card data is passed to a third party site for processing, and never stored by Linux Australia, so there were no credit cards numbers or other data of that sort in the information exposed to the crooks.

Missing from Linux Australia’s otherwise commendably frank breach write-up is:

Information about how the hashed passwords were stored. (This is useful to know, albeit not vital, because it gives a hint as to how successful an offline dictionary attack is likely to be.)

Information about the security hole or holes that let the crooks in. (The document rather conveniently calls it "a currently unknown vulnerability," though clearly it was known to the attackers.)

Information about the RAT and zombie malware that was subsequently installed. (This is handy to know, but again not vital, because RATs and zombies are designed to allow attacks to develop as the crooks see fit, instead of following a predictable pattern.)

Usefully, the Linux Australia crew did publish a list entitled, "What steps were taken to prevent the threat of a similar breach in the future?"

We suggest you take a look at this list.

Even though some of the steps sound rather obvious, most security precautions seem that way in hindsight.

The thing is, even though the steps proposed by Linux Australia aren’t hard to do, they are very easy not to do.

Don’t use the "life’s too short" excuse: these guys are Linux gurus, and they got caught out.

In particular, take notice of this precaution:

The new host will have a far more rigorous operating system updating schedule applied to it.

Even if the exploit used by the crooks in this case really was a zero-day (an attack known only to the crooks, and for which no patch was available), that’s no excuse for being tardy with patches.

Firstly, most attacks don’t use zero-days to get in.

Secondly, even when crooks use a zero-day to get in, they often rely on additional, already-known, security holes to complete their attack.

Patch early, patch often!

Microsoft Challenges Court Order To Turn Over E-Mail in Dublin Datacenter

Microsoft last week filed a legal brief challenging a court order that is forcing the company to turn over a customer’s e-mails stored in a foreign datacenter.

The brief, filed April 8 with the United States Court of Appeals for the Second Circuit, seeks to argue last summer’s court order that Microsoft must turn over the messages from the customer, who is suspected in an alleged drug-related matter. The identity of the suspect is not known and Microsoft said at the time of the ruling, which was upheld by Judge Loretta Preska, that it would appeal the order.

A number of major technology companies last year had filed briefs in support of Microsoft’s appeal including Apple, AT&T, Cisco and Verizon, along with the Electronic Frontier Foundation, noting that the outcome promises to set a precedent for all U.S.-based cloud providers storing data abroad.

"Settled doctrine makes this Court’s job simple: Because laws apply only domestically unless Congress clearly provides otherwise, the statute is properly read to apply only to electronic communications stored here, just as other countries’ laws regulate electronic communications stored there," according to the brief, which Microsoft published. "Even if the Government could use a subpoena to compel a caretaker to hand over a customer’s private, sealed correspondence stored within the United States, however, it cannot do so outside the United States without clear congressional authorization."

Brad Smith, Microsoft’s general counsel and executive vice president for legal and corporate affairs, indicated in a blog post that he’s confident the company will prevail. "As we stated in our brief, we believe the law is on the side of privacy in this case, he said. "This case is about how we best protect privacy, ensure that governments keep people safe and respect national sovereignty while preserving the global nature of the Internet."

Smith also argued that the feds are long overdue in evaluating electronic privacy laws. "While there are many areas where we disagree with the government, we both agree that outdated electronic privacy laws need to be modernized," he said. "The statute in this case, the Electronics Communications Privacy Act, is almost 30 years old, he noted. "That’s an eternity in the era of information technology."

Those differences of course pertain around combatting criminal activities versus protecting privacy. Smith acknowledged that conflict but renewed his plea for the government to find a resolution. "Law enforcement needs to be able to do its job, but it needs to do it in a way that respects fundamental rights, including the personal privacy of people around the world and the sovereignty of other nations," he said. "We hope the U.S. government will work with Congress and with other governments to reform the laws, rather than simply seek to reinterpret them, which risks

happening in this case."

U.S. Lawmaker Who’s Pushing Anti-swatting Bill Gets Swatted

Earlier this month, a crowd of 30 gamers having fun at a PlayStation tournament in a New Jersey video game shop suddenly found themselves handcuffed, staring at shotguns and machine guns, and being told by law enforcement to Shut the F up and get the F down and don’t be F-ing stupid.

That was one of a string of recent swatting incidents in New Jersey that’s spurred a lawmaker to propose stiffening the penalties for the crime.

As of this weekend, Assemblyman Paul Moriarty, sponsor of the anti-swatting bill that would increase penalties for the crime, has first-hand experience of it.

On Saturday, Moriarty was ordered out of his house to find himself facing guns and cops in flak jackets.

Moriarty told NJ.com that he was at home, working on his tax return, when he got a call from police dispatch, asking if everything was OK at his house.

He said everything was fine and asked why they were concerned. That’s when the caller told him that police had received a report of a shooting at his house.

Then, the dispatcher asked Moriarty to describe what he was wearing and to step outside.

This is what happened next, he told NJ.com:

I look out my front door. There’s six cop cars. They have the street closed off. They have helmets, flak jackets and rifles. I walk out and walk towards them. They motion me to keep walking towards them. The minute I walked out the door, I was still on the phone with the dispatch person, I said ’I think I’ve just been swatted.’ It just then occurred to me what happened.

Swatting is the practice of making bogus emergency calls, as a prank or as revenge, with the hopes of getting armed law enforcement or other emergency responders to descend on a victim.

Its origins are in prank calls to emergency services, but in the past few years swatting has become more embedded in the gamer community, with critics of GamerGate, gamers who live-stream on Twitch.TV, and others falling victim.

Moriarty’s bill, introduced in November, would increase penalties for "false public alarm" - also known as swatting - by upgrading the crime from third degree to second degree, boosting the current 3-5 years potential prison time to 5-10 years, and increasing the fine to a maximum of $150,000.

Following the video game store swatting, Moriarty told NJ.com that the

penalties for this crime have got to be strengthened:

Under current law, somebody could end up only serving probation. If you are calling out the SWAT team, and they show up, guns blazing, at some innocent person’s home, and they end up having to break the door down, I think you should go to jail for that. You’re putting lots of people in danger.

Now, he’s thinking that whoever sent the cops to his door must have been inspired by reading his words:

I’m thinking someone read about the bill and some sick, evil person thought it would be funny to send the police to my house on one of these false reports.

He’s not the first person to try to fight swatting via legislation, and he’s not the first such legislator to get swatted himself.

California State Senator Ted Lieu, who was swatted in 2011, sponsored a law that would enable authorities to require perpetrators to bear the "full cost" of emergency services response, which can range up to $10,000.

Teen Charged After Using Teacher’s Admin Password To Access School Computer

A 14-year-old Florida boy has been charged with trespassing on his school’s computer system after he shoulder-surfed a teacher typing in his password, used it without permission to trespass in the network, and tried to embarrass a teacher he doesn’t like by swapping his desktop wallpaper with an image of two men kissing.

The Tampa Bay Times reports that the eighth-grader was arrested on Wednesday for "an offense against a computer system and unauthorized access", which is a felony.

Sheriff Chris Nocco said that the teen logged onto the network of a Pasco County School District school on 31 March using an administrative-level password without permission.

Many who read the news have expressed outrage at the idea of overreach by the school and law enforcement.

But it turns out that there’s less overreach here than meets the eye. In fact, it sounds like the boy has been treated as befits a kid doing dumb things.

It’s not like he was flung into jail, though initial news accounts mistakenly reported that the boy was brought to a nearby juvenile detention center.

In fact, a spokesman for the Pasco County Sheriff’s Office told Network World that the student was not detained. Rather, he was questioned at the school before being released to his mother.

His sentence remains to be seen, but at this point, it’s looking like the boy isn’t going to suffer much more than a 10-day school suspension and what sheriff’s detective Anthony Bossone says is likely to be "pretrial

intervention" by a judge with regards to the felony charge, the Tampa Bay Times reports.

When the newspaper interviewed the student at home, he said that he’s not the only one who uses that password. Other students commonly log into the administrative account to screen-share with their friends, he said.

It’s a well-known trick, the student said, since the password was a snap to remember: it’s just the teacher’s last name, which the boy says he learned by watching the teacher type it in.

The sheriff says that the student didn’t just access the teacher’s computer to pull his wallpaper prank.

He also reportedly accessed a computer with sensitive data - the state’s standardized tests - while logged in as an administrator.

Those are files he well could have viewed or tampered with, though he denies having done so.

Nocco says that’s the reason why this can’t be dismissed as being just a bit of fun:

Even though some might say this is just a teenage prank, who knows what this teenager might have done.

The boy says he was on the computer with standardized tests because he didn’t realize it lacked a camera, so he hopped onto another computer:

I logged out of that computer and logged into a different one and I logged into a teacher’s computer who I didn’t like and tried putting inappropriate pictures onto his computer to annoy him.

He told the newspaper:

If they’d have notified me it was illegal, I wouldn’t have done it in the first place. But all they said was ’You shouldn’t be doing that.’

But here’s the thing: this is actually the second time he’s been caught.

Last year, the boy was one of multiple students who got in trouble for inappropriately accessing the school’s system. He was suspended for three days.

Should the school be taken to task for being lax on security?

Well, yes.

A commenter on Ars Technica’s writeup of the story who identifies themself as a school’s systems administrator - "friblo" - said that there’s nothing surprising here, given tech understaffing:

Schools are generally extremely understaffed technically which makes it difficult to put fires out, much less enforce good password policies. Most schools in my area (rural, decently well funded) have 1 tech for every 750-1000 computers.

It’s not fair to blame schools for a lack of technical savvy when tech troops are so thin on the ground.

But picking a secure password isn’t all that hard, and it doesn’t require calling in IT ninjas.

In fact, it doesn’t cost schools one measly nickel of their already strained budgets to watch this short, jargon-free video on how to pick a proper password.

Yes, the school’s staff are obviously guilty of using feeble passwords. But that doesn’t excuse this student for repeated naughtiness.

Knowingly using a prohibited system for his own kicks is unacceptable, just as it’s wrong to pick up a colleague’s phone and send a bogus message, or to "borrow" a friend’s credit card number to buy something that will look embarrassing on his or her statement.

Accessing a prohibited system is illegal for good reasons.

It can lead to the theft of security or trade secrets, software piracy, economic espionage, financial institution fraud, or to knocking essential systems offline, which can jeopardize public safety and/or cause millions in damages.

School is where kids should be learning not only that accessing off-limit data is illegal, but why.

They should be learning both what ethical computer behaviour looks like, and what happens to those who choose to act unethically, whether it’s by changing their grades to straight As, or writing taunting messages on a rival school’s calendar - both which resulted in felony charges, in spite of sounding like mere schoolboy pranks.

ISP’s Ordered To Hand Over Names and Addresses of Illegal File Sharers

Australian internet service providers (ISPs) have been ordered to hand over names, emails and residential addresses of people who’ve allegedly pirated the movie The Dallas Buyers Club.

In what’s being called a landmark case in the ongoing battle between pirates and big media companies, the Federal Court on Tuesday ordered six ISPs to fork over 4726 unique IP addresses.

The Hollywood studio that won the court case said that the 2013 film was shared by those IP addresses via BitTorrent, a peer-to-peer file transfer protocol for sharing large amounts of data over the internet.

The affected ISPs include the country’s second-largest provider, iiNet, as well as Internode, Adam Internet, Amnet Broadband, Wideband and ISPs Dodo.

They’ve been ordered to hand over contact information of those who allegedly committed the copyright breach by seeding the movie.

According to News.com.au, Voltage - the parent company of Dallas Buyers Club LLC - tracked down the alleged file sharers by using technology that detects and retraces copyright infringement.

The software used to unmask the infringers is called "Maverick Monitor".

According to ZDNet, anyone sharing the film, even just a few kilobytes, may well have have been identified by the software.

That’s proof enough, Justice Nye Perram said in his ruling:

I am comfortably satisfied that the downloading of a sliver of the film from a single IP address provides strong circumstantial evidence that the end user was infringing the copyright in the film.

When the case was heard in February, the ISPs objected to the release of customer information, saying that it would constitute a breach of privacy and open the door to what’s known in the US as "speculative invoicing".

Speculative invoicing is when copyright holders launch court actions or send threatening letters demanding thousands of dollars in punitive fines, over and above what the copyright holder lost out on by somebody illegally downloading a movie.

Justice Perram is well aware of the possibility of speculative invoicing and addressed it in his ruling, which dictates that the customer information be released on the condition that it be used only to recover compensation for the copyright infringement.

He’s going to make sure that alleged infringers don’t get badgered by threatened lawsuits or onerous fees by requiring that he look over the studio’s correspondence before it contacts the identified BitTorrent users.

The BBC quotes the ruling:

I will also impose a condition on the applicants that they are to submit to me a draft of any letter they propose to send to account holders associated with the IP addresses which have been identified.

But that doesn’t necessarily mean that file sharers won’t feel some sting, he said, which is fine by him:

It is not beyond the realm of possibilities that damages of a sufficient size might be awarded under this provision in an appropriately serious case in a bid to deter people from the file-sharing of films.

ZDNet reports that Voltage vice president Michael Wickstrom told the court that the company would be selective about its targeting if it’s allowed to send letters and would likely not go after targets that make the company look bad, such as pensioners, schools, or those in defence.

Online forums such as Slashdot have been abuzz with talk of whether this judgment portends an end to the days of anonymous pirating, and what measures might be taken to get onto BitTorrent in a private way that shields identity.

BitTorrent doesn’t offer anonymity to users. It’s possible to obtain IP addresses of all current and possibly previous participants in a swarm from the tracker, the computer that coordinates file distribution.

Alleged infringers won’t be faced with defending themselves or atoning for their piracy sins any time soon, since it will take some time for the ISPs to find the records - if they in fact still have them.

Also, alleged pirates will be able to challenge whatever claims Voltage

makes in its letters. An IP address in one home may be shared with many people, and it’s not clear that a residential address and email address are sufficient to identify who infringed.

It could get tricky tracking down the guilty party, Perram said, though the specific downloaded titles could help:

Of course, it was possible that the account holders might have some insight into who the end user using BitTorrent might have been. In some cases, this might be straightforward, such as in homes with only two occupants having access to the internet connection. In other cases, it might not be too difficult for the account holder to work out who the downloader was. In many homes, the identity of the film may itself provide some insight into the identity of the file sharer.

The audiences for Cinderella and American Sniper would have few common members (hopefully).

Is DARPA’s Memex Search Engine A Google-killer?

The history of computing features a succession of organisations that looked, for a while at least, as if they were so deeply embedded in our lives that we’d never do without them.

IBM looked like that, and Microsoft did too. More recently it’s been Google and Facebook.

Sometimes they look unassailable because, in the narrow territory they occupy, they are.

When they do fall it isn’t because somebody storms that territory, they fall because the ground beneath them shifts.

For years and years Linux enthusiasts proclaimed "this will be the year that Linux finally competes with Windows on the desktop!", and every year it wasn’t.

But Linux, under the brand name Android, eventually smoked Microsoft when ’Desktop’ gave way to ’Mobile’.

Google has been the 800-pound gorilla of web search since the late 1990s and all attempts to out-Google it have failed. Its market share is rock solid and it’s seen off all challengers from lumbering tech leviathans to nimble and disruptive startups.

Google will not cede its territory to a Google clone but it might one day find that its territory is not what it was.

The web is getting deeper and darker and Google, Bing and Yahoo don’t actually search most of it.

They don’t search the sites on anonymous, encrypted networks like Tor and I2P (the so-called Dark Web) and they don’t search the sites that have either asked to be ignored or that can’t be found by following links from other websites (the vast, virtual wasteland known as the Deep Web).

The big search engines don’t ignore the Deep Web because there’s some

impenetrable technical barrier that prevents them from indexing it - they do it because they're commercial entities and the costs and benefits of searching beyond their current horizons don't stack up.

That's fine for most of us, most of the time, but it means that there are a lot of sites that go un-indexed and lots of searches that the current crop of engines are very bad at.

That's why the US's Defence Advanced Research Projects Agency (DARPA) invented a search engine for the deep web called Memex.

Memex is designed to go beyond the one-size-fits-all approach of Google and deliver the domain-specific searches that are the very best solution for narrow interests.

In its first year it's been tackling the problems of human trafficking and slavery - things that, according to DARPA, have a significant presence beyond the gaze of commercial search engines.

When we first reported on Memex in February, we knew that it would have potential far beyond that. What we didn't know was that parts of it would become available more widely, to the likes of you and me.

A lot of the project is still somewhat murky and most of the 17 technology partners involved are still unnamed, but the plan seems to be to lift the veil, at least partially, over the next two years, starting this Friday.

That's when an initial tranche of Memex components, including software from a team called Hyperion Gray, will be listed on DARPA's Open Catalog.

The Hyperion Gray team described their work to Forbes as:

Advanced web crawling and scraping technologies, with a dose of Artificial Intelligence and machine learning, with the goal of being able to retrieve virtually any content on the internet in an automated way.

Eventually our system will be like an army of robot interns that can find stuff for you on the web, while you do important things like watch cat videos.

More components will follow in December and, by the time the project wraps, a "general purpose technology" will be available.

Memex and Google don't overlap much, they solve different problems, they serve different needs and they're funded in very different ways.

But so were Linux and Microsoft.

The tools that DARPA releases at the end of the project probably won't be a direct competitor to Google but I expect they will be mature and better suited to certain government and business applications than Google is.

That might not matter to Google but there are three reasons why Memex might catch its eye.

The first is not news but it's true none the less - the web is changing and so is internet use.

When Google started there was no Snapchat, Bitcoin or Facebook. Nobody

cared about the Deep Web because it was hard enough to find the things you actually wanted and nobody cared about the Dark Web (remember FreeNet?) because nobody knew what it was for.

The second is this statement made by Christopher White, the man heading up the Memex team at DARPA, who's clearly thinking big:

The problem we're trying to address is that currently access to web content is mediated by a few very large commercial search engines - Google, Microsoft Bing, Yahoo - and essentially it's a one-size fits all interface...

We've started with one domain, the human trafficking domain ... In the end we want it to be useful for any domain of interest.

That's our ambitious goal: to enable a new kind of search engine, a new way to access public web content.

And the third is what we've just discovered - Memex isn't just for spooks and G-Men, it's for the rest of us to use and, more importantly, to play with.

It's one thing to use software and quite another to be able to change it. The beauty of open source software is that people are free to take it in new directions - just like Google did when it picked up Linux and turned it into Android.

Windows XP Clings to No. 2 Spot as Windows 10 Gets Closer

Windows XP continues its descent among desktop operating systems, though it's far from dead and buried.

Looking at the overall Web traffic for desktop operating systems across the globe, Net Applications gave XP a 16.9 percent share for the month of March, a hefty drop from the 19.1 percent recorded in February.

Though XP's grip on the market continues to loosen, it remains the No. 2 most-used operating system based on Net Application's Web stats, beating Windows 8 and 8.1 and their collective share of 14 percent. Windows 8.1 took the third spot with a 10.5 percent share, leaving Windows 8 in fifth place with just 3.5 percent.

Windows 7 holds the top spot, with a share of 58 percent.

The enduring hold of the 13-year-old Windows XP on PC users underscores the challenges Microsoft has faced as it tries to move ahead with new versions of its flagship operating system, which the company says has more than 1.5 billion users around the world. The staying power has even proven resistant to Microsoft's end of support for XP a year ago, which put an end to bug fixes and and other patches, leaving users more vulnerable to security threats.

There are ripple effects as well. Last month, chipmaker Intel slashed nearly $1 billion off its quarterly revenue outlook, in large part because small and midsize businesses have been reluctant to upgrade from Windows XP - a popular but now 13-year-old operating system. PC makers, such as Hewlett-Packard, Lenovo and Acer, would also feel a pinch from

slower refreshes from Windows XP.

The next leap forward comes this summer when Microsoft plans to release Windows 10, which among other things aims to avoid the missteps of Windows 8 and to provide a consistent software experience across devices including desktops, laptops, smartphones and even Internet of Things gear including ATMs and ultrasound machines.

With Windows 10 arriving soon, what choices are available to those who want to upgrade?

For users of Windows 7 and Windows 8.1, Microsoft is offering free upgrades to Windows 10 for the first year. That means you can download and install Windows 10 for free and directly upgrade your existing PC. But users still running Windows XP or Vista won't be able to ugprade their PCs directly to Windows 10, according to Microsoft. That leaves them the choice of upgrading to Windows 8.1 and then to Windows 10 or simply buying a new PC this summer already equipped with Windows 10.

Currently available as a technical preview, Windows 10 has been showing up as a blip on Net Applications' radar. For March, the new OS took home a share of just under 0.1 percent.

New Algorithm Could Auto-squash Trolls

Ah trolls. A species we know well - those people who bounce around in comments sections flinging language dung all over the intertubes.

Well, that language dung comes in handy when trying to spot a troll, it turns out.

Researchers have found that bad writing is one behaviour of several characteristics that can be crunched in a new algorithm that can predict commenters who'll be banished for trollery.

The researchers, from Stanford and Cornell Universities, say in their paper that their algorithm can pinpoint future banned users (FBUs) with an 80% AUC (Area Under the Curve is a type of accuracy scoring that takes false positives into account).

The researchers analysed troll behaviour in the comments sections of three online news communities: the general news site CNN.com, the political news site Breitbart.com, and the computer gaming site IGN.com.

Those sites all have a list of users who've been banned for antisocial behavior: a total of over 10,000 antisocial lab rats.

The sites also have all of the messages posted by the banned users throughout their period of online activity, giving the researchers a handy pool of subject material, they said:

Such individuals are clear instances of antisocial users, and constitute 'ground truth' in our analyses.

The algorithm compares messages posted by users who were ultimately banned against messages posted by users who were never banned, managing to spot FBUs after analysing as few as 5 to 10 posts.

They found clear differences between the two groups:

Trolls' posts are more garbled. The researchers used several readability tests, including the Automated Readability Index (ARI), to gauge how easy it is to read a given chunk of text. They found that nearly all of the 10,000 FBUs studied displayed a lower perceived standard of literacy and/or clarity than the median for their host groups, with even that lackluster standard dropping as they neared their ultimate ban.

Trolls swear more. Not only do they swear more, they're also pretty decisive. They don't tell others to "perhaps" go P off and F themselves, since they don't tend to use conciliatory/tentative words such as "could", "perhaps", or "consider" - words that research has found tend to minimise conflict.

Trolls are not sunshiney people. At least, they tend to stay away from positive words.

Trolls tend to wander. They have a tendency to veer off-topic.

Trolls like to dig in for protracted flame wars. This behaviour differs by community - on Breitbart and IGN, FBUs tend to reply to others' posts, but on CNN, they're more likely to start new discussions. But across all communities, they like to drag others into fruitless discussion, getting significantly higher replies than regular users and protracting the discussion by chiming in far more frequently per thread than normal people.

The communities themselves aren't entirely off the hook when it comes to being turned into troll playgrounds, the researchers say.

[Communities] may play a part in incubating antisocial behavior. In fact, users who are excessively censored early in their lives are more likely to exhibit antisocial behavior later on. Furthermore, while communities appear initially forgiving (and are relatively slow to ban these antisocial users), they become less tolerant of such users the longer they remain in a community. This results in an increased rate at which their posts are deleted, even after controlling for post quality.

The researchers say the algorithm should be of high practical importance to those who maintain the communities.

But given its 80% accuracy, that still leaves 20% of commenters who could be unfairly tarred and feathered, they admitted.

Fed-up, out-of-patience communities themselves throw gas on the fire by overreacting to minor infractions - which can come off as unfair and cause FBUs to behave even more badly, the researchers say.

As well, the classification of a given user as troll or non-troll could stand to be a lot more nuanced. Feigning ignorance, for example, and asking naive questions might be a troll tactic too subtle to show up on the algorithm's radar.
All of which suggests that patience might be a better approach than auto-squashing trolls, at least for now:

Though average classifier precision is relatively high (0.80), one in five users identified as antisocial are nonetheless misclassified. Whereas trading off overall performance for higher precision and

[having] a human moderator approve any bans is one way to avoid incorrectly blocking innocent users, a better response may instead involve giving antisocial users a chance to redeem themselves.

=~=~=~=